Digital signature procedure based on blind signatures for use in cryptography and electronic payment systems

Publication number:	FR2775399
Publication date:	1999-08-27
Inventor:	TRAORE JACQUES; DE SOLAGES AYMERIC
Applicant:	FRANCE TELECOM (FR)
Classification:	
- international:	***H04L9/32;*** **H04L9/32;** (IPC1-7): H04L9/32; G07F7/08
- european:	H04L9/32S
Application number:	FR19980002196 19980224
Priority number(s):	FR19980002196 19980224

Abstract of **FR2775399**

In a message exchange between an emitter and a user, the message is digitally signed. By allowing the emitter to see a part of the message, the complete blindness of the signatory is avoided and he is permitted to see a part of the signature. The signature is called blind. The user sends only a part of the message to the emitter sign. The emitter can then incorporate the part of the signal in the information elements necessary for recognition of the signal which once produced, can only be verified, with the help of the entire message, of which a part has been seen by the emitter.

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 775 399**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **98 02196**

(51) Int Cl^6 : **H 04 L 9/32**, G 07 F 7/08

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 24.02.98.

(30) **Priorité** :

(43) **Date de mise à la disposition du public de la demande** : 27.08.99 Bulletin 99/34.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *FRANCE TELECOM Société anonyme* — FR.

(72) **Inventeur(s)** : TRAORE JACQUES et DE SOLAGES AYMERIC.

(73) **Titulaire(s)** :

(74) **Mandataire(s)** : SOCIETE DE PROTECTION DES INVENTIONS.

(54) PROCEDE DE SIGNATURE NUMERIQUE BORGNE.

(57) Procédé de signature numérique.

Par un échange d'informations entre un émetteur et un utilisateur, mettant en jeu un message, on constitue une signature. En permettant à l'émetteur de prendre connaissance d'une partie du message, on évite la cécité complète du signataire et on lui permet de reconnaître une partie de la signature. La signature obtenue est alors dite " borgne ".

Application au paiement électronique.

FR 2 775 399 - A1

PROCEDE DE SIGNATURE NUMERIQUE BORGNE

DESCRIPTION

Domaine technique

La présente invention a pour objet un procédé de signature numérique. Ce procédé comprend, d'une part, une opération de retrait et d'autre part, une opération de présentation de la signature.

L'invention trouve une application notamment dans le paiement électronique.

Etat de la technique antérieure

Un concept particulier de signature numérique, dit signature aveugle, a été introduit par D. CHAUM dans un article intitulé "Blind Signatures for Untraceable Payments" publié dans "Proceedings of CRYPTO'82, Plenum Press, 1983, pp. 199-203.

Un protocole de signature aveugle est un protocole cryptographique mettant en jeu deux entités, un "utilisateur" et un "émetteur", l'utilisateur faisant signer un message à l'émetteur, de telle manière que ce dernier n'obtienne aucune information sur le contenu du message qu'il signe. De plus, après avoir signé plusieurs messages, l'émetteur est incapable, à la vue d'une signature qu'il a contribué à créer, de déterminer lors de quelle exécution du protocole cette signature a été obtenue.

Les protocoles de signature aveugle sont utilisés dans des applications nécessitant l'anonymat, telles que les élections électroniques ou la monnaie électronique. Dans les systèmes de paiement électronique anonyme, l'expression "pièce électronique" désigne une donnée signée numériquement par la banque (l'émetteur de monnaie électronique). La fonction de

signature utilisée par la banque détermine la valeur faciale de la pièce. Lors d'une phase dite de "retrait", l'utilisateur (le client) achète ces pièces électroniques. Pour garantir l'anonymat, les pièces retirées par l'utilisateur doivent être inconnues de la banque. A cette fin, cette dernière signe de manière aveugle des données que l'utilisateur crée de manière secrète. L'utilisateur se trouve ainsi en possession de pièces valides que la banque elle-même est incapable d'associer à l'utilisateur qui les a retirées. L'anonymat est parfait. Le paiement correspond ensuite à un transfert de pièces électroniques du client au commerçant. Ce dernier contacte alors la banque (cas du paiement en ligne), laquelle conserve, dans sa base de données, toutes les pièces non expirées qui ont déjà été dépensées, pour s'assurer que les pièces qui lui sont présentées n'ont pas déjà été dépensées lors d'une transaction antérieure. Les commerçants déposent ensuite à la banque, lors de la phase dite de "remise", les pièces qu'ils ont reçues en paiement, pour compensation de leur valeur.

Divers modes de mise en oeuvre d'une signature aveugle ont été développés et décrits. On peut en trouver des exemples notamment dans l'article de D. CHAUM et T.P. PEDERSEN, intitulé "Wallet Databases with Observers", publié dans Proceedings of Crypto'92, Lecture Notes in Computer Science, vol. 740, Springer Verlag, pp. 89-105, ainsi que dans l'article de T. OKAMOTO, intitulé "Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes", publié dans Proceedings of Crypto'92, Lecture Notes in Computer Science, vol. 740, Springer Verlag, pp. 31-53. Le protocole d'authentification de Schnorr, dont dérivent les protocoles de signature aveugle utilisés dans les articles ci-dessus, est lui-même

décrit dans l'article de C.P. SCHNORR, intitulé "Efficient Signature Generation by Smart Cards", publié dans Journal of Cryptology, 4(3) 1991, pp. 161-164.

Dans le protocole d'authentification de SCHNORR, et dans les schémas de signature aveugle qui en dérivent, l'émetteur E choisit au hasard une clef secrète S_E, calcule une clef publique $P = g^{S_E}$, où g est un élément générateur connu de tous. Puis l'entité E publie sa clef publique P de façon que chacun la connaisse comme étant associée à l'identité de E. La clef publique P ne permet pas de retrouver la clef secrète S_E que seul E connaît. En effet, la fonction exponentielle , qui permet de passer de S_E à P, est difficilement inversible (la taille des paramètres est choisie de façon que le temps nécessaire pour retrouver S_E à partir de P soit trop long pour les ordinateurs disponibles à l'époque de la mise en oeuvre du protocole).

Dans le schéma d'authentification de SCHNORR, l'entité E prouve à une entité utilisatrice U qu'elle connaît la clef secrète S_E sans toutefois révéler celle-ci. Cette preuve constitue pour E un moyen de s'authentifier auprès de l'utilisateur U.

Ce protocole d'authentification comprend une première opération où l'émetteur choisit au hasard un nombre x dans le groupe Zq, c'est-à-dire dans le corps des entiers modulo q où q est un nombre premier (autrement dit x est compris entre 1 et $q-1$) et élève son générateur g à la puissance x pour constituer un nombre t qui va lancer le protocole d'authentification. Ce nombre t est transmis à l'utilisateur qui poursuit le protocole en choisissant au hasard un nombre c dans Zq et en le transmettant à l'émetteur, qui calcule alors une réponse appropriée en utilisant sa clef secrète S_E

que lui seul connaît. Cette clef n'est évidemment pas transmise en l'état mais masquée par le nombre x que l'émetteur seul connaît. La réponse est alors $y = x - cS_E$.

L'utilisateur traite cette réponse en calculant, g^y qui n'est autre que $g^{(x-cS_E)}$, soit $g^x g^{-cS_E}$. L'utilisateur peut calculer aussi P^c, soit g^{cS_E}, de sorte que le produit $g^y P^c$ est égal à $g^x g^{-cS_E} g^{cS_E}$, c'est-à-dire finalement t.

La vérification de l'égalité entre t et $g^y P^c$ prouve à l'utilisateur que l'émetteur connaît bien la clef secrète S_E. Par ailleurs, cette preuve est apportée sans que la clef S_E ait été révélée à l'utilisateur. Le protocole peut donc se répéter autant de fois que l'on veut, à condition de changer le nombre x à chaque fois.

On peut illustrer un tel protocole par un tableau, (représentation qui sera utilisée constamment dans la suite de la description) dans lequel la notation Zq désigne le corps des entiers modulo q, les flèches horizontales symbolisent la transmission de nombre(s) d'une entité à l'autre, une équation avec un point d'interrogation au-dessus du signe égal ($\stackrel{?}{=}$) signifie que l'entité vérifie que les deux membres de l'égalité sont bien égaux. Avec ces conventions, le protocole d'authentification qui vient d'être décrit, peut être représenté par le Tableau I ci-après.

E		U
clef secrète : S_E		
clef publique : $P = g^{S_E}$		
choisit x dans Zq		
calcule $t = g^x$		
	$\xrightarrow{t}$	
		choisit c dans Zq
	$\xleftarrow{c}$	
$y=x-cS_E$		
	$\xrightarrow{y}$	
		$\hat{t}=g^y P^c$

Tableau I

Ce protocole constitue une preuve de connaissance par l'émetteur de la clef secrète. On peut lier cette preuve à un message m, de façon à ce que ce protocole constitue en même temps une signature σ du message m. En toute rigueur, l'émetteur E ne mériterait pas vraiment le nom de "signataire", car il ne peut être tenu pour responsable du message signé m puisqu'il l'ignore. C'est néanmoins la terminologie usuelle.

Un schéma de signature aveugle de ce type peut être illustré par le Tableau II avec les mêmes conventions, où m est le message à signer. Dans ce schéma, l'utilisateur choisit en outre au hasard deux nombres u et v dans Zq, et calcule un nombre t à partir du nombre $\hat{t}$ qu'il a reçu de l'émetteur, du générateur g de l'émetteur qui est connu de tous et de la clef publique P de ce même émetteur et en utilisant les nombres u et v comme exposants, soit $t = \hat{t} g^v P^u$.

L'utilisateur choisit ensuite un nombre c, dit challenge, compris dans Zq et masque ce challenge en lui soustrayant le nombre u connu de lui seul pour obtenir un challenge masqué $\hat{c} = c - u$. L'utilisateur transmet le challenge masqué $\hat{c}$ à l'émetteur.

E		U
clef secrète : S_E		*message :* m
clef publique : $P = g^{S_E}$		
choisit x dans Zq		
calcule $\hat{t} = g^x$		
	$\xrightarrow{\hat{t}}$	
		choisit u, v dans Zq
		calcule $t = \hat{t} g^v P^u$
		calcule $c = H(t, m)$
		calcule $\hat{c} = c - u$
	$\xleftarrow{\hat{c}}$	
calcule $\hat{y} = x - \hat{c} S_E$		
	$\xrightarrow{\hat{y}}$	
		calcule $y = \hat{y} + v$
		$t = g^y P^c$
		obtient la signature $\sigma = (y, c, m)$

Tableau II

Dans ce protocole, H est une fonction de hachage (ou de condensation) connue de tous. La signature σ finalement obtenue est constituée par l'ensemble des nombres y, c et m. Une telle signature ne peut être reconnue par l'émetteur qui ne peut calculer ni y, ni c, puisqu'il ignore les paramètres de masquage u et v et ne peut reconnaître le message m, qu'il n'a jamais vu.

Les applications de la signature aveugle sont assez limitées, sauf à lui associer d'autres protocoles. Le but de la présente invention est justement de remédier à cet inconvénient pour élargir le champ d'application de tels protocoles.

Exposé de l'invention

A cette fin, l'invention propose un procédé dans lequel l'émetteur prend connaissance d'une partie du message à signer. Sa cécité n'est donc plus totale mais partielle. On dira que le signataire, et par extension la signature, est "borgne".

De façon plus précise, la présente invention a pour objet un procédé de retrait de signature numérique dans lequel une entité dite "émetteur" (E) échange avec une entité dite "utilisateur" (U) des informations selon un protocole permettant à l'utilisateur d'obtenir une signature (σ) d'un message (μ) à l'élaboration de laquelle l'émetteur a collaboré mais sans que ce dernier puisse la retrouver à partir des éléments connus de lui lors de ces échanges ni la lier, lorsqu'elle lui est présentée a posteriori, au retrait dont elle provient si l'émetteur a émis plusieurs signatures, ce procédé étant caractérisé par le fait que l'utilisateur ne communique à l'émetteur qu'une partie (M) du message à signer, partie que ce dernier incorpore dans des éléments d'information nécessaires à l'élaboration de la signature, qui une fois produite ne peut être vérifiée qu'à l'aide du message (μ) entier, dont la partie (M) qui a été vue par l'émetteur.

L'invention a également pour objet un procédé de présentation d'une signature borgne obtenue par le procédé qui vient d'être défini, à une entité tierce dite "tiers" qui vérifie cette signature.

Exposé détaillé de modes particuliers de réalisation

Dans tous ce qui suit on se placera dans un groupe Gq cyclique d'ordre q, où q est un entier premier, et dans lequel la détermination du logarithme est un problème difficile : trouver x, s'il existe, tel que $a^x=b$ est difficile.

Un exemple de retrait de signature borgne conforme à l'invention va d'abord être décrit. Il s'apparente au schéma de signature aveugle exposé plus haut (Tableau II). Mais selon l'invention, le message à signer comprend deux parties, une premier partie M qui sera rendue visible à l'émetteur et une seconde partie m qui restera invisible (ou masquée) pour celui-ci. Dans l'exemple décrit, l'émetteur E possède une clef secrète S_E et deux clefs publiques P_1, P_2 associées à cette même clef secrète par deux nombres générateurs g_1 et g_2 ; on a donc :

$$P_1 = g_1^{S_E} \qquad P_2 = g_2^{S_E}$$

A la différence du schéma de signature aveugle décrit plus haut (Tableau II), l'utilisateur transmet à l'émetteur, au début du procédé, la partie visible M du message et l'émetteur insère cette partie du message dans ses paramètres, par exemple en calculant un nombre générateur g_M défini à partir des générateurs g_1 et g_2 par $g_M = g_1^M g_2$.

C'est ce nombre g_M qui servira alors à calculer le nombre $\hat{t}$ et non plus le nombre g comme dans le tableau II. En tirant encore un nombre x au hasard, l'émetteur calculera g_M^x et non plus g^x.

La suite des opérations restera sensiblement la même, à cette différence que l'utilisateur devra reconstituer le nombre t en tenant compte de la

particularité de $\hat{t}_M$ (et non plus de t). Les opérations détaillées sont alors celles du tableau III.

E		U
		message μ :
clef secrète : S_E		*partie visible* : M
clefs publiques : P_1, P_2		*partie invisible* : m
générateurs : g_1, g_2		
$P_1 = g_1^{S_E}$, $P_2 = g_2^{S_E}$		
	$\xleftarrow{M}$	
calcule $g_M = g_1^M g_2$		
choisit x dans Zq		
calcule $\hat{t}_M = g_M^x$		
	$\xrightarrow{\hat{t}_M}$	
		calcule $P_M = P_1^M P_2$
		choisit u, v dans Zq
		calcule $t_M = \hat{t}_M g_M^v P_M^u$
		calcule $c=H(t_M, M, m)$
		calcule $\hat{c} = c - u$
	$\xleftarrow{\hat{c}}$	
calcule $\hat{y} = x - \hat{c}S_E$		
	$\xrightarrow{\hat{y}}$	
		calcule $y = \hat{y} + v$
		$t_M = g_M^y P_M^c$
		obtient la signature $\sigma=(y, c, M, m)$

Tableau III

La signature obtenue est formée des deux nombres y et c, connus du seul utilisateur, et du message $\mu=(M, m)$, dont la première partie seule, M, est connue de l'émetteur.

L'exploitation de cette signature s'effectue par un protocole de présentation auprès d'une troisième entité dit "Tiers" et notée T. Ce tiers calcule d'abord le produit $g_M^y P_M^c$, autrement dit $\left(g_1^M g_2\right)^y \cdot \left(P_1^M P_2\right)^c$. Ce calcul est possible puisque le tiers reçoit y, c et M par la signature et qu'il connaît les clefs publiques P_1, P_2 ainsi que les générateurs g_1, g_2 de l'émetteur. Ce produit, qui n'est autre que le nombre t_M calculé par l'utilisateur lors du retrait de la signature, permet au tiers de reformer la fonction $H(t_M, M, m)$ et de vérifier si le résultat est bien le nombre c contenu dans la signature.

Ce protocole de présentation est illustré par le tableau IV suivant :

U		T
$\sigma=(y, c, M, m)$	$\xrightarrow{(y, c, M, m)}$	$t_M = g_M^y P_M^c$ $c = H(t_M, M, m)$

Tableau IV

Le procédé qui vient d'être décrit peut s'appliquer au paiement électronique. Dans le cas d'un système de paiement, l'émetteur émet des signatures représentant des pièces électroniques. Les utilisateurs les emploient pour payer auprès des commerçants, lesquels jouent le rôle de tiers vérificateurs. La présentation de la pièce électronique peut donc s'assimiler à un paiement. Ces pièces doivent pouvoir être utilisées de façon anonyme, comme la monnaie fiduciaire classique, ce qui impose l'utilisation de signatures aveugles.

Avec une signature borgne conforme à l'invention, la partie visible (M) du message peut contenir diverses informations, comme un montant maximal, les dates d'émission et d'expiration de la pièce, un nombre maximal d'utilisations autorisées. La partie invisible m peut contenir des données relatives au paiement, notamment l'identité du tiers (T), la date et l'heure, la référence du bien acheté.

Pour remédier au problème de rendu de monnaie, une solution possible est d'émettre des pièces de montant faible, ou même correspondant à la granularité de la monnaie (par exemple, des pièces de 1 centime exclusivement). Cependant, cette solution obligerait à émettre des quantités importantes de pièces. Une autre solution consiste à émettre des pièces utilisables plusieurs fois, et constituées d'une signature borgne. La partie visible M du message peut alors contenir le nombre maximal d'utilisations autorisé et le montant maximal autorisé pour l'ensemble de ces utilisations.

Le procédé de signature borgne qui vient d'être décrit peut être combiné avec tout procédé de signature "juste" dans lequel des traces du retrait et/ou de la présentation peuvent être insérées dans les protocoles afin, le cas échéant, pour pouvoir retrouver l'utilisateur d'une pièce donnée ou les pièces d'un utilisateur donné. En particulier, le procédé de signature borgne de l'invention peut être combiné à un procédé particulier de signature juste tel que celui qui est décrit et revendiqué dans la demande de brevet déposée le jour même du dépôt de la présente demande par le présent Demandeur, et intitulée "Procédé de signature numérique juste".

REVENDICATIONS

1. Procédé de retrait de signature numérique, dans lequel une entité dite "émetteur" (E) échange avec une entité dite "utilisateur" (U) des informations selon un protocole permettant à l'utilisateur d'obtenir une signature (σ) d'un message (μ) à l'élaboration de laquelle l'émetteur a collaboré mais sans que ce dernier puisse la retrouver à partir des éléments connus de lui lors de ces échanges ni la lier, lorsqu'elle lui est présentée a posteriori, au retrait dont elle provient si l'émetteur a émis plusieurs signatures, ce procédé étant caractérisé par le fait que l'utilisateur ne communique à l'émetteur qu'une partie (M) du message (μ) à signer, partie que ce dernier incorpore dans des éléments d'information nécessaires à l'élaboration de la signature, qui une fois produite ne peut être vérifiée qu'à l'aide du message (μ) entier, dont la partie (M) qui a été vue par l'émetteur.

2. Procédé selon la revendication 1, dans lequel :

- l'émetteur (E) possède une première clef publique P_1, un premier élément générateur public g_1, et une clef secrète S_E, avec $P_1 = g_1^{S_E}$, l'émetteur possédant encore une seconde clef publique P_2 et un second élément générateur public g_2, avec $P_2 = g_1^{S_E}$, les nombres P_1, P_2, g_1 et g_2 étant connus de l'utilisateur (U),
- pour incorporer la partie (M) du message (μ) qui lui est communiquée dans des éléments d'information nécessaires à l'élaboration de la signature, l'émetteur calcule un élément g_M défini par :

$$g_M = g_1^M g_2 ,$$

- l'émetteur commençant ensuite le protocole de signature en choisissant au hasard un nombre entier x, en calculant un nombre $\hat{t}_M$ égal à g_M^x, et en transmettant ce nombre $\hat{t}_M$ à l'utilisateur.

3. Procédé selon la revendication 2, dans lequel l'utilisateur (U), ayant reçu le nombre $\hat{t}_M$, calcule un nombre P_M égal au produit $P_1^M P_2$, choisit au hasard deux nombres entiers u et v, calcule un nombre t_M défini par :

$$t_M = \hat{t}_M g_M^v P_M^u ,$$

calcule un challenge (c) qui est une fonction de ce nombre t_M et du message $(\mu=(M, m))$, soit $c=H(t_M, M, m)$ où H est une fonction de hachage connue, puis calcule un challenge masqué $(\hat{c})$ égal à $c-u$ et transmet ce challenge masqué $(\hat{c})$ à l'émetteur.

4. Procédé selon la revendication 3, dans lequel l'émetteur (E), pour calculer la réponse appropriée au challenge masqué reçu $(\hat{c})$, calcule un nombre $\hat{y}$ égal à $\hat{y} = x - \hat{c} S_E$ et transmet ce nombre $\hat{y}$ à l'utilisateur (U).

5. Procédé selon la revendication 4, dans lequel, l'utilisateur (U) traite la réponse reçue $(\hat{y})$ en calculant un nombre y défini par $y = \hat{y} + v$, calcule la quantité $g_M^y P_M^c$ et vérifie que cette quantité calculée coïncide avec le nombre t_M déjà calculé, la signature (σ) du message pouvant être alors constituée par l'utilisateur en regroupant la réponse traitée y, le challenge c et le message $(\mu=(M, m))$ $(\sigma=(y, c, M, m))$.

6. Procédé de présentation d'une signature obtenue selon la revendication 5, comprenant les opérations suivantes :

- l'utilisateur transmet la signature ($\sigma=(y, c, M, m)$) à un tiers (T),
- le tiers (T), à partir des nombres y, M et c pris dans la signature (σ) ainsi que des nombres générateurs g_1, g_2 et des clefs publiques P_1, P_2 de l'émetteur (E) calcule un nombre t_M égal à $(g_1^M g_2)^y . (P_1^M P_2)^c$,
- à partir du nombre t_M ainsi calculé et des première et seconde parties du message (M, m) prises dans la signature, le tiers (T) calcule la quantité $H(t_M, M, m)$ et vérifie que cette quantité coïncide bien avec le challenge (c) pris dans la signature reçue.

7. Procédé selon la revendication 6, dans lequel la production d'une signature représente la création d'une pièce de monnaie électronique au profit de l'utilisateur (U) et la présentation de la signature représente un paiement électronique auprès du tiers (T).

8. Procédé selon la revendication 7, dans lequel la partie (M) du message transmise à l'émetteur peut contenir des informations comme un montant maximal, une date d'émission, une date d'expiration, un nombre maximal d'utilisations autorisées.

9. Procédé selon la revendication 7, dans lequel la partie (m) du message non transmise à l'émetteur contient des données relatives au paiement, notamment l'identité du tiers (T), la date et l'heure, la référence du bien acheté.

10. Procédé selon la revendication 1, dans lequel on insère dans la signature (σ) une information

permettant de retrouver la trace de son retrait auprès de l'émetteur (E).

11. Procédé selon la revendication 10, dans lequel le tiers (T) auquel la signature (σ) est présentée inclut, dans la signature, une information permettant de retrouver la trace de la présentation de la signature.

2775399

RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 557186
FR 9802196

DOCUMENTS CONSIDERES COMME PERTINENTS

Categorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
X	MIYAZAKI S ET AL: "A more efficient untraceable E-cash system with partially blind signatures based on the discrete logarithm problem" FINANCIAL CRYPTOGRAPHY. SECOND INTERNATIONAL CONFERENCE, FC'98 PROCEEDINGS, FINANCIAL CRYPTOGRAPHY. SECOND INTERNATIONAL CONFERENCE, FC'98. PROCEEDINGS, ANGUILLA, 23-25 FEB. 1998, pages 296-308, XP002086619 ISBN 3-540-64951-4, 1998, Berlin, Germany, Springer-Verlag, Germany * page 297, ligne 10 - page 298, ligne 25; figure 1 *	1
X	ABE M ET AL: "How to date blind signatures" ADVANCES IN CRYPTOLOGY - ASIACRYPT'96 INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATIONS OF CRYPTOLOGY AND INFORMATION SECURITY. PROCEEDINGS, ADVANCES IN CRYPTOLOGY - ASIACRYPT '96. , 3 novembre 1996, pages 244-251, XP002086620 ISBN 3-540-61872-4, 1996, Berlin, Germany, Springer-Verlag, Germany * page 245, ligne 23 - page 247, ligne 4 *	1

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

H04L

1

Date d'achèvement de la recherche	Examinateur
3 décembre 1998	Holper, G

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C13)